CLAIMS

We claim:

1. An information distribution system comprising:

a key management server for managing secret keys and public keys corresponding to given attribute values;

a user terminal for accessing said key management server to obtain attribute secret keys generated based on said secret keys, said attribute secret keys corresponding to attributes of said user terminal; and

a provider terminal for generating an encrypted content that can be decrypted by said user terminal having said attribute secret keys corresponding to given attributes by means of said public keys,

wherein said provider terminal distributes said encrypted content and said user terminal decrypts said encrypted content decryptable by means of said attribute secret keys of its own.

2. The information distribution system according to claim 1, wherein said provider terminal distributes said encrypted content without specifying said user terminal that is to receive said encrypted content.

3. The information distribution system according to claim 1, wherein said user terminal sends a set of attribute values indicating attributes of its own to said key management server; and

said key management server generates said attribute secret keys unique to said user terminal based on, among said secret keys managed by said key management server, secret keys corresponding to the attribute values sent from said user terminal and sends said attribute secret keys to said user terminal.

4. A server comprising:

a key storage for storing secret keys and public keys corresponding to predetermined attribute values;

an attribute secret key generator for obtaining a set of given attribute values and generating attribute secret keys corresponding to said set of attribute values based on secret keys corresponding to said attribute values among said secret keys stored in said key storage; and

a sending/receiving unit for receiving said set of attribute values from a given user terminal and sending said attribute secret keys generated by said attribute secret key generator to said user terminal.

5. The server according to claim 4, wherein said attribute secret key generator generates said attribute secret keys by using a protocol implementing oblivious transfer.

6. An information processing apparatus comprising:

a criteria key generator for obtaining public keys corresponding to attribute values indicating attributes of a recipient to which a content is to be sent and using said public keys to generate criteria keys that can be decrypted by secret keys corresponding to said public keys;

an encrypted content generator for encrypting said content based on said criteria keys; and

a sending unit for sending said encrypted content without specifying any recipient of said content via a network.

7. The information processing apparatus according to claim 6, wherein said criteria key generator combines, based on predetermined rules, criteria keys corresponding to the individual attribute values encrypted by using public keys corresponding to said individual attribute values to generate a criteria key for restricting recipients of said content.

8. The information processing apparatus according to claim 6, wherein said criteria key generator generates a session key for encrypting said content and a criteria key for decrypting said session key; and

said encrypted content generator uses said session key to encrypt said content.

9. An information processing apparatus receiving a content distributed over a network, comprising:

a sending/receiving unit for accessing a key management server managing secret keys and public keys corresponding to given attribute values to receive attribute secret keys corresponding to attributes established for said information processing apparatus, said attribute secret keys being generated based on said secret keys; and

a decryptor for obtaining an encrypted content and decrypting said content based on said attribute secret keys.

10. The information processing apparatus according to claim 9, wherein said sending/receiving unit sends a set of attribute values established for said information processing apparatus to said key management server and receives said attribute secrete keys generated based on said set of attribute values from said key management server.

11. A program for controlling a computer to generate a decryption key for decrypting information encrypted with a given public key, said program causing said computer to implement the functions of claim 4.

12. The program according to claim 11, wherein said computer-implemented function of generating said attribute secret key generates said attribute secret keys by using a protocol implementing oblivious transfer.

13. A program for controlling a computer to encrypt and distribute a given content, causing said computer to implement the functions of claim 6.

14. The program according to claim 13, wherein said computer-implemented function of generating said criteria key combines, based on predetermined rules, criteria keys corresponding to the individual attribute values encrypted by using public keys corresponding to said individual attribute values to generate a criteria key for restricting recipients of said content.

15. A program for controlling a computer to receive content distributed over a network, causing said computer to implement the functions of:

accessing a key management server managing secret keys and public keys corresponding to given attribute values to receive attribute secret keys corresponding to attributes established for said information processing apparatus according to claim 6, said attribute secret keys being generated based on said secret keys; and

obtaining the encrypted content and decrypting said encrypted content based on the attribute secret keys.

16. A storage medium containing a program in computer readable form for controlling a computer to generate decryption key for decrypting information encrypted with a given public key, said program causing said computer to implement the functions of claim 4.

17. A storage medium containing a program in computer readable form for controlling a computer to encrypt and distribute a given content, said program causing

said computer to implement the functions of claim 6.

18. A storage medium containing a program in computer readable form for controlling a computer to receive a content distributed over a network, said program causing said computer to implement the functions of claim 9.

19. A key distribution method for controlling a computer to generate and distribute a decryption key for decrypting information encrypted with a given public key, comprising the steps of:

generating n secret keys and n public keys corresponding to said secret keys and storing said secret keys and public keys in a given storage;

obtaining information about k (≤n) secret keys selected at random by a given client from among said n secret keys stored in said storage;

reading said k secret keys corresponding to information about the obtained secret keys from said storage and using a protocol for implementing oblivious transfer to generate decryption keys for decrypting information encrypted with said k public keys corresponding to the k secret keys; and

providing said generated decryption keys to said client.

20. An information distribution system comprising:

a service provider managing secret keys and public keys for given attribute values; and

a plurality of user terminals for accessing said service provider to obtain attribute secret keys corresponding to attributes of their own, said attribute secret keys being generated based on said secret keys;

wherein, a given one of said user terminals generates an encrypted content and sends said encrypted content to one or more of the other user terminals, said encrypted content being decryptable by said one or more of the other user terminals having said attribute secret keys corresponding to given attributes by means of said public keys; and

said one or more of the other user terminals decrypt said encrypted content decryptable by means of said attribute secret keys of their own.

21. An information distribution system comprising:

a key management server for managing secret keys and public keys for given attribute values; and

a plurality of user terminals for accessing said key management server to obtain attribute secret keys corresponding to attributes of their own, said attribute secret keys being generated based on said secret keys,

wherein a given one of said user terminals generates a group key and sends said group key to ones of the other user terminals and provides a content , said encrypted group key being decryptable by said ones of the other user terminals having said attribute secret keys corresponding to given attributes by means of said public keys, said content being only accessible by using said group key.

22. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing key distribution, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 19.

23. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for key distribution, said method steps comprising the steps of claim 19.

24. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing key distribution, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 20.

25. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing key distribution, the computer readable program code means in said computer program product

comprising computer readable program code means for causing a computer to effect the functions of claim 21.